(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 830 353**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **02 02519**

(51) Int Cl[7] : **G 06 F 17/60**, H 04 L 12/16, 9/32, H 04 Q 7/32, G 06 K 19/10, G 07 C 15/00 // G 06 F 161:00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 28.02.02.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 04.04.03 Bulletin 03/14.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *CP8 Société anonyme* — FR.

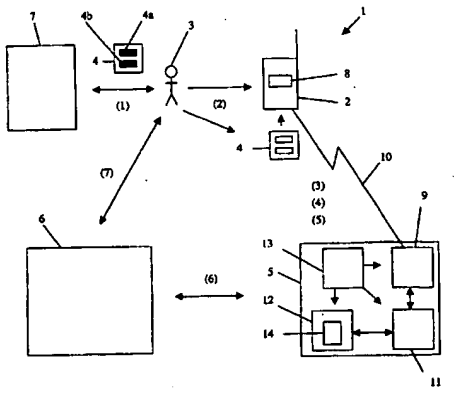
(72) **Inventeur(s) :** PODEUR YVAN.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :**

(54) PROCEDE ET DISPOSITIF DE MISE EN OEUVRE SECURISEE DE JEUX DU TYPE LOTERIE UTILISANT UN TELEPHONE MOBILE.

(57) La présente invention concerne un procédé de mise en oeuvre sécurisée d'un jeu de pari tel qu'un jeu de loterie nécessitant la communication d'une donnée d'un utilisateur (3) à un centre (5) de gestion et utilisant un organe (2) de transmission. Le procédé consiste à transmettre audit centre (5) de gestion ladite donnée obtenue à partir d'un support prépayé par ledit utilisateur et si ladite donnée est retrouvée dans les moyens de stockage du centre de gestion, à valider la participation dudit utilisateur (3) audit jeu.



FR 2 830 353 - A1

PROCEDE ET DISPOSITIF DE MISE EN ŒUVRE SECURISEE DE JEUX DU TYPE LOTERIE UTILISANT UN TELEPHONE MOBILE

La présente invention concerne un procédé et un système de mise en œuvre sécurisée de jeux nécessitant un pari tel qu'un jeu de loterie utilisant un téléphone mobile.

DOMAINE TECHNIQUE

La dénomination "carte" sera utilisée dans la description qui suit pour désigner un système embarqué à puce électronique.

Le téléphone mobile peut être un téléphone portatif ou un terminal plus complexe, par exemple un terminal cumulant les fonctionnalités de téléphone et d'organiseur ou de calculette.

La présente invention s'applique plus particulièrement au domaine des téléphones mobiles comprenant un organe de lecture ou plus que l'on appellera ci-après lecteur auxiliaire recevant une carte dite auxiliaire. Le lecteur auxiliaire se présente habituellement sous la forme d'un lecteur de carte à puce classique. Il comporte pour ce faire une fente dans laquelle la carte à puce est introduite le temps d'une transaction.

De plus en plus, des fournisseurs de service cherchent à offrir de nouvelles applications embarquées sur les téléphones mobiles : ils fournissent à la fois ladite application embarquée sur le téléphone mobile et le service associé sur le serveur.

Ainsi, les fournisseurs de jeux nécessitant un pari d'un joueur tel que par exemple un jeu de loterie cherchent aujourd'hui à offrir la possibilité audit joueur d'émettre un pari à partir de son téléphone mobile.

TECHNIQUE ANTERIEURE

Il existe actuellement des jeux de loterie tels que le jeu « koodpo » (marque déposée) accessible depuis un téléphone mobile consistant à demander à un utilisateur de choisir des numéros et de les transmettre au moyen de son téléphone mobile. Si les numéros sortent au tirage, l'utilisateur est notifié du montant de ses gains.

Cependant, aucun paiement (outre celui de l'appel) n'est requis de la part de l'utilisateur : le jeu est entièrement gratuit. Aucune transaction financière n'est requise. L'utilisateur rentre directement les numéros sur son téléphone après avoir appelé le service de loterie en question. L'utilisateur est astreint à une grille par jour : le résultat du tirage est donné le lendemain matin. L'utilisateur doit s'inscrire et communiquer des informations personnelles afin de recevoir le prix du tirage pour lequel il est gagnant : l'utilisateur ne conserve donc pas l'anonymat comme dans les jeux informatisés de loterie existant.

L'invention vise à pallier les inconvénients des dispositifs et systèmes de l'art connu tout en satisfaisant aux besoins qui se font sentir.

Un but de la présente invention est d'offrir aux utilisateurs de téléphone mobile les mêmes possibilités de jeux que les jeux informatisés de loterie existants.

Un autre but de la présente invention est de proposer un procédé permettant d'authentifier un pari d'un joueur tout en assurant l'anonymat de ce dernier.

Un autre but de la présente invention est de proposer un procédé permettant d'assurer la confidentialité et la sécurisation des échanges entre le téléphone mobile et le service de jeux, notamment lors de transactions financières telles que celle ayant pour but de payer le bulletin joué.

RESUME DE L'INVENTION

La présente invention concerne un procédé de mise en œuvre sécurisée d'un jeu de pari tel qu'un jeu de loterie nécessitant la communication d'une donnée d'un utilisateur à un centre de gestion et utilisant un organe de transmission, caractérisé en ce qu'il consiste à transmettre audit centre de gestion ladite donnée obtenue à partir d'un support prépayé par ledit utilisateur et si ladite donnée est retrouvée dans des moyens de stockage du centre de gestion, à valider la participation dudit utilisateur audit jeu.

La présente invention concerne également le centre de gestion apte à mettre en œuvre ce procédé.

La présente invention porte sur un support comprenant des moyens de mémorisation d'informations et apte à être inséré dans un organe de transmission, caractérisé en ce qu'il comprend au moins une zone masquée susceptible d'être découverte de manière définitive sur laquelle est inscrite une donnée et en ce que les moyens de mémorisation comprennent des paramètres propres à un ou plusieurs types de jeu de pari tel que jeu de loterie et/ou des éléments divers susceptibles d'être utilisés lors dudit jeu.

DESCRIPTION SOMMAIRE DES DESSINS

L'invention va maintenant être décrite de façon plus détaillée en se référant au dessin annexé illustrant schématiquement une forme de réalisation du système selon l'invention dans lequel les étapes du procédé selon l'invention sont mises en évidence.

MANIERE DE REALISER L'INVENTION

La présente invention s'applique, bien que non exclusivement, aux téléphones mobiles suivant la norme "GSM". En effet, une des normes les plus utilisées en Europe est la norme de transmission "GSM" (acronyme pour "Groupe spécial Systèmes Mobiles publics de radiocommunications fonctionnant dans la bande des 900 MHz"). On doit bien comprendre cependant que l'invention ne saurait se résumer à cette seule norme. Notamment, elle peut trouver application dans le cadre des normes en cours de développement telles "GPRS" ou "UTMS" ou autre.

Le système 1 selon l'invention comprend un téléphone 2 mobile d'un utilisateur 3. Le téléphone 2 mobile est susceptible de recevoir une carte 4. La carte 4 est un système embarqué à puce électronique, par exemple une carte à puce. La carte 4 est de type carte à gratter : sa surface présente au moins une zone masquée, en l'espèce deux zones 4a et 4b, susceptibles d'être découvertes par grattage ou par tout autre moyen connu. Les zones 4a et 4b sont appelées zones à gratter. Les informations inscrites dans les zones à gratter sont une donnée appelée ci-après identifiant et une information obtenue à l'aide d'un processus de calcul cryptographique à partir d'un ou plusieurs éléments divers tels que l'identifiant, appelée ci-après signature ; les informations peuvent être inscrites de manière séparée sur les deux zones 4a, 4b ou sur plus de deux zones ou de manière regroupée sur une seule zone. Les informations peuvent également être concaténées ou mélangées suivant certaines règles ou autres dans la ou lesdites zones. L'identifiant représente le numéro de la carte lors de sa fabrication. L'identifiant et la signature permettent d'assurer la sécurité des échanges entre l'utilisateur et un centre de gestion 5 et plus précisément l'authentification de l'utilisateur auprès du centre de gestion tout en lui permettant de conserver son anonymat et la vérification que la carte utilisée par l'utilisateur est une des cartes émises par le centre de gestion.

Selon une forme particulière de l'invention, la carte 4 comprend plusieurs zones à gratter. La signature est constituée par l'ensemble ou une partie des zones grattées.

Selon une autre forme particulière de l'invention, la carte 4 comporte plusieurs zones à gratter. Une zone ou un groupe de zones correspond à un jeu. La signature diffère selon le jeu choisi.

La carte 4 comprend des moyens de mémorisation des paramètres d'un jeu donné nécessitant un pari (ou de la combinaison de plusieurs jeux), utilisés par le téléphone mobile, comme il sera vu plus loin, pour transmettre au centre de gestion le type de jeu et de pari et le montant joué, d'informations permettant d'assurer la sécurité entre l'utilisateur et un centre 6 de paiement. Les moyens de mémorisation peuvent également contenir des informations optionnelles telles que la manière de jouer (un seul ou plusieurs paris émis).

La carte 4 est distribuée aux utilisateurs 3 par un vendeur de carte 7. Le vendeur de carte 7 se présente sous tout type de forme à savoir un kiosque, tout type de magasin, supermarché, un bar tabac ou autre. La carte 4 peut être remise à un utilisateur par tout autre moyen tel que par exemple un envoi par courrier.

Le téléphone 2 comporte une application 8 embarquée dont la fonction est de permettre la saisie du pari de l'utilisateur 3 et la transmission de manière sécurisée dudit pari vers le centre 5 de gestion et de recevoir et communiquer à l'utilisateur la confirmation de sa participation au tirage et les résultats dudit tirage. Le terme "application embarquée" doit être compris dans son sens le plus général. Il concerne naturellement des appliquettes ou programmes similaires, mais aussi englobe toutes sortes de données numériques. L'application 8 est implémentée dans le téléphone 2 ou dans toute carte comprise dans le téléphone 2 telle que par exemple

une carte SIM ou encore pour partie dans le téléphone 2 et pour partie dans une carte.

Le centre 5 de gestion se présente sous la forme d'un serveur comprenant un module 9 d'interface avec un réseau 10 de téléphonie mobile, un module 11 de traitement, des moyens 12 de mémorisation d'informations par exemple une base de données, un module 13 de gestion de sécurité. Les moyens 12 de mémorisation stockent une liste 14 d'identifiants des cartes 4. Le centre 5 de gestion gère le service de paris interactifs avec le téléphone mobile de l'utilisateur : il centralise tous les paris émis pour un tirage donné, confirme auprès des utilisateurs la réception desdits paris, effectue le tirage en question et notifie les résultats du tirage et les gains en découlant au(x) gagnant(s). Le centre de gestion fabrique ou sous-traite la fabrication des cartes 4 qu'il commercialise ensuite auprès des vendeurs 7 de carte.

Le téléphone 2 est relié au centre 5 de gestion au travers du réseau 10 de téléphonie mobile. Le terme « réseau » doit être compris dans son sens le plus général. Il inclut les composants de transmission proprement dits du réseau (sous-systèmes de radio transmission, câbles de transmissions, faisceaux hertziens, sous-systèmes "filaires" terrestres, etc.), mais aussi tous les systèmes raccordés au réseau de téléphonie mobile (stations de base, contrôleurs de station, commutateurs, annuaires, etc., et, de façon plus générale, tous systèmes de traitement informatique de données et serveurs raccordés au réseau).

L'application 8 de la carte 4 d'abonné communique au travers du réseau 10, avec une ou plusieurs applications installées sur le serveur 7, via le canal des messages courts. La technologie dite de « service à messages courts » (service dit « GSM-Data ») est connue sous le sigle « SMS » (pour « Short Message Service »). Ce canal est indépendant de celui de la voix et est standardisé par la norme "GSM". Les applications, qu'elles soient installées sur le téléphone ou une carte du téléphone ou sur

le serveur, peuvent à la fois envoyer et recevoir des informations, appelées messages courts qui contiennent du texte ou des données en format binaire. Les messages courts sont codifiés à l'aide de caractères de contrôle (identifiant (PID: Protocole IDentifier), adresse de l'émetteur, nombre d'octets,...).

Il est à noter que selon la forme de réalisation, selon le type de réseau choisi, les technologies de communication peuvent différer. Le terme « message » est utilisé dans ce qui suit pour désigner un message court ou tout autre type de message.

Le système 1 comprend un centre 6 de paiement des gains réalisés par l'utilisateur 3. Le centre de paiement peut se présenter sous diverses formes : par exemple, le centre de paiement peut être une entité faisant partie de l'organisme de jeu, distincte ou non du centre 5 de gestion, une banque, les gains réalisés étant directement versés sur un compte de l'utilisateur, le vendeur de carte 7 ...

Le procédé selon l'invention comprend les étapes suivantes.

Lors de la fabrication des cartes 4, le centre 5 de gestion inscrit ou fait inscrire l'identifiant sur l'une des zones masquées 4a et la signature sur l'autre zone 4b. Le centre 5 inscrit l'ensemble des identifiants des cartes produites sur la liste 14 d'identifiants. Il est à noter que l'identifiant, et l'identifiant uniquement peut être inscrit en clair sur la carte. L'identifiant inscrit sur la carte 4 distribuée est connu du centre de gestion.

Le centre 5 de gestion distribue les cartes 4 auprès des vendeurs 7 de carte.

L'utilisateur 3 achète une carte 4 (Etape 1 sur la figure 1) auprès du vendeur 7 de carte correspondant au(x) jeu(x) auquel il souhaite participer. La carte 4 est prépayée auprès du vendeur 7 de carte qui la délivre ce qui

évite toute transaction monétaire entre l'utilisateur et le centre de gestion : le montant de la somme versée par l'utilisateur au vendeur de carte pour obtenir la carte est stockée dans les moyens de mémorisation de la carte de manière à permettre à l'utilisateur de jouer plusieurs fois. Si l'utilisateur ne souhaite jouer qu'une fois avec la carte qu'il acquiert, le montant n'a pas besoin d'être mémorisé.

De plus, l'utilisateur décide du moment où il émet son pari. Il peut effectuer son pari quelques minutes avant le tirage depuis n'importe quel lieu géographique : un pari émis par un utilisateur n'est validé par le centre de gestion qu'une fois la clôture des paris pour un tirage donné entérinée.

Lorsque l'utilisateur 3 souhaite participer à un tirage, il prend connaissance de l'identifiant et de la signature de la carte 4 en grattant les zones 4a, 4b masquées. L'utilisateur 3 insère (Etape (2) sur la figure 1) la carte 4 dans son téléphone 2 et lance un menu interactif lui permettant d'effectuer son pari. L'application 8 gère ledit menu et les échanges avec l'utilisateur.

L'utilisateur commence par saisir l'identifiant et la signature dont il a pris connaissance. Il est à noter que des interfaces de reconnaissance ou des périphériques optionnels peuvent être prévus pour lire les informations inscrites sur la carte 4.

Un menu contextuel adapté propose une liste de choix prédéfinis de manière conviviale. L'utilisateur peut également préparer son pari de manière manuelle sans accéder à un menu particulier. Le profil de l'utilisateur, et par exemple la manière préférée de jouer de l'utilisateur 3 est susceptible d'être préenregistrée dans une application du téléphone 2 (application du téléphone ou d'une carte incluse dans le téléphone telle qu'une carte SIM) ou du centre 5 de gestion. Des icônes et signaux sonores agrémentent le parcours du menu.

Le choix d'un tirage est proposé à l'utilisateur sous forme d'un calendrier ou de sélections à choix multiples. L'utilisateur sélectionne le tirage souhaité.

Il est demandé à l'utilisateur une grille de numéros sélectionnés pour le tirage. L'utilisateur 3 choisit des numéros dans une grille affichée ou saisit une série de numéros. L'application 8 peut effectuer à la demande de l'utilisateur une présélection automatique de ses numéros favoris. L'application 8 peut également comprendre un mécanisme de type connu permettant de tirer des numéros de manière aléatoire et proposer à l'utilisateur des numéros choisis au hasard au moyen dudit mécanisme. Un récapitulatif est affiché au fur et à mesure de la saisie des numéros par l'utilisateur.

Le montant du pari peut être saisi par l'utilisateur ou automatiquement obtenu à partir des paramètres de la carte 4. L'application 8 prépare un message destiné au centre de gestion à partir des données saisies par l'utilisateur et de données contenues dans la carte 4 et le téléphone 2. Le message comprend par exemple les champs suivants :

Identifiant et numéro d'appel
Signature
Pari
Date et horaire du tirage
Montant du pari
Anonymat

Dans l'exemple suivant, l'identifiant et la signature sont fournies par l'utilisateur. Le pari peut provenir de plusieurs origines : soit la grille est entièrement ou partiellement choisie et fournie par l'utilisateur, soit le pari n'est en fait qu'une demande par l'utilisateur qu'un pari soit fait pour lui par

le centre de gestion, soit le pari provient du mécanisme de tirage aléatoire du téléphone, soit la grille est fournie par le profil enregistré dans le centre de gestion ou le téléphone. La date et l'horaire du tirage ne font partie des données préparées que si la technologie SMS n'est pas utilisée ; en effet, ces informations sont envoyées automatiquement dans les messages SMS. Le montant est donné par la carte mais est optionnel comme vu précédemment. L'anonymat est une donnée fournie par l'utilisateur pour indiquer s'il souhaite ou ne souhaite pas rester anonyme. Le numéro d'appel est donné par le téléphone ou l'application 8 et permet au centre de gestion d'envoyer un accusé de réception à l'utilisateur. Dans le cas où le champ Anonymat du message indique que l'utilisateur souhaite rester anonyme, toute information concernant l'utilisateur tel que le numéro d'appel est détruite après utilisation. De plus, l'utilisateur n'est pas forcément le propriétaire du téléphone : il est le propriétaire de la carte prépayée lui permettant d'effectuer son pari. Il reste anonyme même s'il gagne puisque la carte prépayée n'est pas nominative : le gagnant est identifié par la détention de la carte et du certificat renvoyé par le centre de gestion à l'utilisateur comme il sera vu plus loin.

Tout ou partie des informations collectées peuvent être soit optionnelles, soit filtrées, soit pré initialisées par l'utilisateur, par le téléphone mobile ou par l'application 8.

D'autres informations peuvent être inclues dans le message transmis au centre de gestion pour lui permettre de connaître le profil de l'utilisateur et de dialoguer au mieux avec lui par l'intermédiaire de son téléphone. Les informations sont les suivantes :

- le type de téléphone 2 de l'utilisateur afin d'interpréter la saisie des données transmises au centre de gestion d'une manière propre audit téléphone et de permettre au centre de gestion de renvoyer une réponse au téléphone au format qui convient ;

- le lieu et le pays d'émission du message par l'utilisateur afin de déterminer la provenance des messages reçus et de considérer les législations en vigueur dans certains pays ;
- le réseau 10 utilisé afin de favoriser des partenariats entre opérateurs et centre de gestion et de permettre une tarification particulière ;
- le format du message transmis, la langue utilisée, des caractéristiques spécifiques au message (alphabet, devises ...) ;
- le profil de l'utilisateur de manière à enregistrer ses préférences et ses habitudes de jeux, répertorier les besoins des utilisateurs en général.

Après confirmation par l'utilisateur, le téléphone 2 transmet ledit message au centre 5 de gestion qui en accuse réception (Etape (3) sur la figure 1). Le module 9 d'interface du centre 5 reçoit les messages et les transmet au module 11 de traitement. Le module de traitement retrouve les informations pertinentes dans le message reçu.

Si une erreur est détectée dans le message, un message d'erreur est renvoyé à l'utilisateur. Le centre de gestion et plus particulièrement le module de traitement vérifie que l'identifiant transmis par le téléphone 2 fait partie de la liste 14 des identifiants valides mémorisés dans les moyens 12 de mémorisation et si tel est le cas raye l'identifiant en question de ladite liste. La liste 14 permet au centre de gestion de détecter des fausses cartes, des identifiants incorrects, parce que ne correspondant à aucun des identifiants des cartes distribuées par le centre de gestion, des identifiants déjà utilisés l'identifiant utilisé étant rayé dans la liste.

Le module de traitement procède ensuite à l'authentification de la carte 4. Pour ce faire, il communique l'identifiant et la signature reçue au module 13 de gestion de sécurité.

La signature inscrite sur la carte 4 est calculée à l'aide d'une clé à partir d'un défi et de l'identifiant. Le défi est fixe ou pseudo aléatoire. Selon une forme avantageuse de l'invention, la signature est produite selon un algorithme, appelé « quartz », protégé en France par le brevet n°2737370 déposé le 27 juillet 1995 par le présent demandeur. De cette manière, la signature est unique et courte : elle comporte de 16 à 20 digits maximum. Elle peut être inscrite dans la zone 4a de la carte à gratter.

Selon une forme particulière de l'invention, certaines parties de la signature ne sont pas transmises, par exemple certains digits parmi les 16 à 20. Les digits absents sont retrouvés par le module 11 de traitement du centre 5 de gestion par toute sorte de processus. De cette manière, la signature est raccourcie et l'utilisateur a moins de digits à saisir.

Les moyens 12 de mémorisation contiennent la liste 14 des identifiants des cartes distribuées associés avec les défis à partir desquels ont été calculés les signatures pour chaque identifiant. Le module 13 de gestion de la sécurité retrouve donc le défi correspondant à l'identifiant en question dans les moyens 12. Une autre solution pour retrouver le défi associé à l'identifiant concerné consiste à utiliser une méthode de calcul donnée.

A partir du défi retrouvé dans les moyens 12 et de l'identifiant reçu, le module 13 calcule la signature au moyen de l'algorithme cryptographique utilisé pour calculer la signature inscrite sur la carte. Le module 13 la compare à celle reçue. Si les signatures correspondent, le module 13 authentifie le pari et en conclut que l'utilisateur a fait son pari à l'aide d'une carte émise par le centre de gestion et jusque là non utilisée. La signature certifie les données transmises au centre de gestion. Le centre de gestion a l'assurance que les données reçues d'un utilisateur proviennent d'une carte 4 achetée par celui-ci et issue dudit centre.

Si aucune erreur n'est détectée, le centre de gestion renvoie un message récapitulatif de confirmation (étape (4) sur la figure 1). Le pari est effectif à l'émission du message récapitulatif de confirmation. Le pari est validé et inscrit au registre des paris. De cette manière, l'utilisateur n'a pas à faire valider son pari auprès du vendeur de carte et le vendeur 7 n'a pas besoin de se munir d'un appareil de validation spécifique au jeu en question.

Le message récapitulatif de confirmation contient un certificat datant et signant la transaction associée à la participation au tirage. Le certificat représente le sceau du centre de gestion certifiant la participation au tirage de l'utilisateur associé à un identifiant donné. Le certificat correspond à une signature du centre de gestion sur l'identifiant et le défi à partir d'un algorithme cryptographique.

L'utilisateur note le certificat et sa grille de numéros transmis. Selon une forme de réalisation particulière, l'utilisateur enregistre dans les moyens de mémorisation de la carte 4 le certificat et la grille en question. Selon une autre forme de réalisation, l'utilisateur enregistre dans des moyens de mémorisation de son téléphone (du téléphone proprement dit ou des cartes qu'il contient telle que la carte SIM) ledit certificat et ladite grille.

Le module 11 de traitement du centre de gestion procède au tirage (étape (5) sur la figure 1) et transmet de manière immédiate à l'utilisateur le résultat du tirage. De manière optionnelle, le centre de gestion notifie à l'utilisateur le montant de ses gains en l'invitant à rejoindre le centre 6 de paiement le plus proche ainsi que des statistiques complétant l'information transmise à l'utilisateur. L'utilisateur sait donc rapidement à l'aide de son téléphone s'il fait partie des gagnants sans recourir à un moyen tel qu'une télévision ou le vendeur de carte qui peut être d'accès difficile ou lointain. Le centre de gestion informe (étape (6) sur la figure 1) également le centre

de paiement des gagnants du tirage en question en lui indiquant le certificat, la grille et l'identifiant desdits gagnants.

Si l'utilisateur a gagné au tirage auquel il a participé, il se rend au centre 6 de paiement (Etape (7) sur le figure 1). Il remet sa grille et sa carte. Si l'identifiant sur la carte correspond à celui reçu du centre de gestion et que les grilles sont identiques, il reçoit le montant de ses gains.

En revanche, si les identifiants ou les grilles ne correspondent pas, le centre de paiement vérifie le certificat du centre de gestion. Si le certificat ne correspond pas, cela signifie que l'utilisateur n'a pas utilisé une carte émise par le centre de gestion et l'utilisateur ne reçoit pas ses gains. En revanche, si le certificat correspond à celui reçu par le centre de paiement, le centre de paiement et le centre de gestion recherchent l'origine de l'erreur sur les identifiants ou les grilles afin de pouvoir remettre au détenteur du certificat concerné les gains correspondants.

Pour que la transaction soit effectuée, que le centre de gestion prenne en compte le pari de l'utilisateur, que l'utilisateur soit assuré de toucher ses gains auprès du centre de paiement, le téléphone mobile doit transmettre au centre de gestion un identifiant et une signature irrévocable.

La sécurité du procédé selon l'invention est assurée par la carte 4 et le certificat retourné par le centre de gestion. La signature apportée par la carte 4 et le certificat sont des preuves de validation pour les deux parties, utilisateur et centre de gestion. : aucune contestation n'est possible.

De plus, si une erreur survient telle qu'une grille mauvaise, une signature ou un identifiant incorrect ou une carte invalide, le centre de gestion en informe l'utilisateur et lui demande de corriger le problème pour représenter une requête valide.

Si la carte 4 a déjà été utilisée, l'utilisateur le détecte facilement à l'aide des zones masquées qui auraient déjà été grattées pour obtenir des informations nécessaires pour la participation à un tirage. L'identifiant du support permet au centre de gestion de détecter une nouvelle transmission de données pour un même identifiant et de garantir ainsi une utilisation unique du support. D'autres moyens peuvent être prévus pour garantir une utilisation unique tel que mémoriser l'identifiant dans la carte et le rayer ou le supprimer de la carte à l'aide par exemple du téléphone une fois l'identifiant fourni par la carte pour être transmis au centre de gestion.

Le système et le procédé selon l'invention permettent à un utilisateur d'effectuer un pari à partir de n'importe quel lieu géographique. De plus, la validation d'un bulletin au niveau international ouvre un plus grand espace de marché et donc une diffusion de jeux à très grande échelle. Les gains seront aussi nettement plus importants et plus attractifs pour un utilisateur.

La présente invention peut se présenter sous tout autre type de forme. A titre illustratif, l'utilisateur effectue son pari à l'aide de tout moyen de communication domestiques ou publics. La validation est réalisée vocalement en ligne.

La présente invention peut recouvrir tout autre type de domaine. En particulier, la carte comprenant des zones masquées dans lesquelles sont inscrites un identifiant et une signature peut être utilisée pour sécuriser tout autre type d'opération.

REVENDICATIONS

1) Procédé de mise en œuvre sécurisée d'un jeu de pari tel qu'un jeu de loterie nécessitant la communication d'une donnée d'un utilisateur (3) à un centre (5) de gestion et utilisant un organe (2) de transmission, caractérisé en ce qu'il consiste à transmettre audit centre (5) de gestion ladite donnée obtenue à partir d'un support prépayé par ledit utilisateur et si ladite donnée est retrouvée dans des moyens de stockage du centre de gestion, à valider la participation dudit utilisateur (3) audit jeu.

2) Procédé selon la revendication 1, caractérisé en ce qu'il consiste à conserver la trace de la transmission de ladite donnée de manière à ne pas valider la participation dudit utilisateur si ladite donnée a déjà été transmise au centre (5).

3) Procédé selon l'une des revendications 1 à 2, caractérisé en ce qu'il consiste à transmettre audit centre (5) de gestion en plus de ladite donnée, une information calculée à partir de ladite donnée et/ou d'un ou plusieurs autres éléments au moyen d'un processus de calcul cryptographique, ladite information étant obtenue à partir dudit support (4).

4) Procédé selon la revendication 3, caractérisé en ce l'algorithme cryptographique est de type quartz.

5) Procédé selon l'une des revendications 3 ou 4, caractérisé en ce qu'il consiste à renvoyer à l'organe de transmission (2) dudit utilisateur un certificat calculé à l'aide d'un processus de calcul cryptographique à partir de ladite donnée et/ou de ladite information et/ou d'un ou plusieurs autres

éléments, certificat indiquant audit utilisateur que sa participation a été validée.

6) Procédé selon l'une des revendications 3 ou 4, caractérisé en ce que le centre de gestion ou tout autre composant calcule une information appelée signature au moyen d'un algorithme cryptographique à partir de la donnée reçue et/ou d'un élément appelé défi, défi associé à ladite donnée reçue et retrouvé par le centre de gestion dans des moyens de mémorisation, et en ce que le centre de gestion ne valide la participation de l'utilisateur que si ladite signature calculée correspond à ladite information reçue.

7) Procédé selon l'une des revendications 1 à 6, caractérisé en ce que l'organe (2) de transmission utilise et/ou transmet en plus de ladite donnée au centre (5) de gestion des informations contenues dans ledit support (4) inséré dans l'organe de transmission ou autres et/ou des informations saisies dans l'organe de transmission (2) par l'utilisateur (3) et/ou des informations pré enregistrées dans ledit organe de transmission (2).

8) Procédé selon la revendication 5, caractérisé en ce que le centre de gestion transmet les résultats du jeu à l'utilisateur et à un centre (6) de paiement et communique ladite donnée et ledit certificat audit centre de paiement.

9) Centre de gestion apte à mettre en œuvre le procédé selon l'une des revendications 1 à 8.

10) Organe de transmission tel qu'un téléphone mobile apte à mettre en œuvre le procédé selon l'une des revendications 1 à 8.

11) Support comprenant des moyens de mémorisation d'informations et apte à être inséré dans un organe (2) de transmission,

caractérisé en ce qu'il comprend au moins une zone masquée susceptible d'être découverte de manière définitive sur laquelle est inscrite une donnée et en ce que lesdits moyens de mémorisation comprennent des paramètres propres à un ou plusieurs types de jeu de pari tel qu'un jeu de loterie et/ou des éléments divers susceptibles d'être utilisés lors de la mise en œuvre dudit jeu.

12) Support selon la revendication 11, caractérisé en ce qu'il comprend au moins une zone masquée susceptible d'être découverte de manière définitive sur laquelle est inscrite une information obtenue à l'aide d'un processus de calcul cryptographique à partir de ladite donnée et/ou d'un ou plusieurs autres éléments.

13) Support selon la revendication 12, caractérisé en ce que ladite donnée et/ou ladite information est(sont) inscrit(es) sur une ou plusieurs zones masquées données, la donnée et/ou l'information étant elle-même(elles-même) inscrit(es) dans chacune des zones de manière normale, mélangée ou cryptée.

14) Programme d'ordinateur comprenant des instructions de code de programme pour l'exécution d'étapes du procédé selon l'une des revendications 1 à 8 lorsque ledit programme est exécuté dans un système informatique ou équivalent.

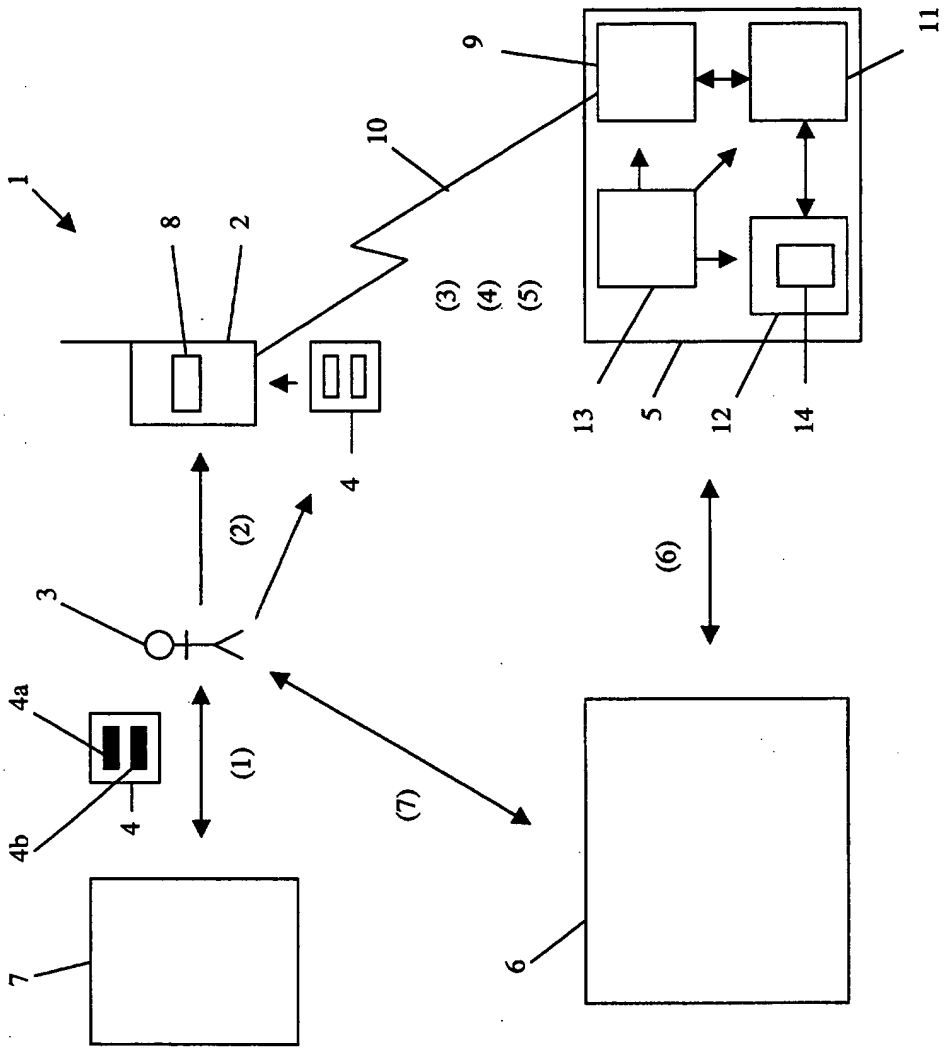


FIG. 1

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2830353

N° d'enregistrement national

FA 615504
FR 0202519

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	FR 2 809 578 A (SAGEM) 30 novembre 2001 (2001-11-30)	1,7,9-14	G06F17/60 H04L12/16
A	* page 2, ligne 19 - ligne 25 * * page 5, ligne 21 - page 7, ligne 32 * * abrégé; figure 1 *	3-6,8	H04L9/32 H04Q7/32 G06K19/10 G07C15/00
X	CH 691 649 A (SYLVAIN VICTOR NAHUM) 31 août 2001 (2001-08-31)	1,9,10, 14	
A	* colonne 1, ligne 34 - ligne 50 * * colonne 5, ligne 23 - ligne 50 * * abrégé; revendication 6; figures 1,4 *	3,4,7	
X	US 6 028 920 A (CARSON JOHN T) 22 février 2000 (2000-02-22)	1,2,9, 10,14	
A	* colonne 1, ligne 29 - ligne 66 * * colonne 10, ligne 16 - ligne 39 * * abrégé; revendication 1; figures 7,8 *	3,11-13	
A	WO 99 42964 A (SWISSCOM AG ;STADELMANN ANTON NIKLAUS (CH)) 26 août 1999 (1999-08-26) * page 2, ligne 11 - page 3, ligne 17 *	1-14	

DOMAINES TECHNIQUES RECHERCHÉS (Int.Cl.7)

G07F
G06F

1

Date d'achèvement de la recherche	Examinateur
28 août 2002	Reule, D

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0202519 FA 615504

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 28-08-2002
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication		Membre(s) de la famille de brevet(s)	Date de publication
FR 2809578	A	30-11-2001	FR	2809578 A1	30-11-2001
CH 691649	A	31-08-2001	CH	691649 A5	31-08-2001
US 6028920	A	22-02-2000	US	6134309 A	17-10-2000
			AU	9585898 A	23-04-1999
			EP	1039981 A1	04-10-2000
			WO	9916566 A1	08-04-1999
WO 9942964	A	26-08-1999	AT	215718 T	15-04-2002
			AU	2262599 A	06-09-1999
			BR	9908097 A	31-10-2000
			CA	2318801 A1	26-08-1999
			WO	9942964 A1	26-08-1999
			DE	59901116 D1	08-05-2002
			EP	1057147 A1	06-12-2000
			US	6416414 B1	09-07-2002

EPO FORM P0465